Exhibit A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

CAROLE CORRALEJO, individually and on behalf of those similarly situated, Plaintiff, v. **BAYMARK HEALTH SERVICES, INC,** Defendant.	Case No.: 4:25-cv-00174 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Carole Corralejo ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant BayMark Health Services, Inc. ("BayMark" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of Defendant BayMark's failures to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiff's and Class Members' (defined below) sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant is an organization that provides medical treatment and/or employment to individuals, including Plaintiff and Class Members. According to a "Notice of Data Privacy Incident" posted on Defendant's website, a data breach occurred on its network between

September 24, 2024 and October 14, 2024 (the "Data Breach").[1]

3. Due to Defendant's data security failures which resulted in the Data Breach, cybercriminals were able to target Defendant's computer systems and exfiltrate highly sensitive and personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and Class Members. As a result of this Data Breach, the Private Information of Plaintiff and Class Members remains in the hands of those cybercriminals.

4. Defendant's website notice states that, upon learning of the Data Breach, it "took steps to secure our systems, launched an investigation with the assistance of third-party forensic experts, and notified law enforcement."[2] However, despite apparently learning of the Data Breach on or about November 5, 2024 and determining that Private Information was involved in the breach, Defendant did not begin sending notices to the victims of the Data Breach (the "Notice of Data Breach Letters") until January 8, 2025.

5. The Private Information compromised in the Data Breach included current and former patients' PII and PHI, including Plaintiff's. This Private Information included, but is not limited to: patient names, Social Security number, driver's license number, date of birth, services received, dates of service, insurance information, treating provider, and treatment and/or diagnostic information.[3]

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information with which it was entrusted for either treatment or employment or

[1] https://baymark.com/notice-of-data-privacy-incident/ (last visited February 13, 2025)
[2] *Id.*
[3] *Id.*

both.

7. Plaintiff brings this class action lawsuit on behalf of herself and all other similarly situated persons to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and failing to include in that belated and inadequate notice precisely what specific types of information were accessed and taken by cybercriminals.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that network in a dangerous condition.

9. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

10. In addition, Defendant failed to properly monitor the computer network and systems that housed Private Information. Had Defendant properly monitored its computer network and systems, it would have discovered the massive intrusion sooner rather than allowing

cybercriminals almost a month of unimpeded access to the PII and PHI of Plaintiff and Class Members.

11. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including: opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all other similarly situated individuals whose Private Information was accessed during the Data Breach.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of

contract, (iv) breach of implied contract, (v) breach of fiduciary duty; (vi) unjust enrichment; (vii) invasion of privacy; (viii) declaratory and injunctive relief; (ix) violation of California's Unfair Competition Law ("UCL"), Cal Bus. & Prof. Code § 17200, *et seq*.; and (x) violation of the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

PARTIES

18. Plaintiff Carole Corralejo is and at all times mentioned herein was an individual citizen of the State of California and was Defendant's patient. Plaintiff Corralejo received notice of the Data Breach dated January 8, 2025. A redacted version of Plaintiff's letter is attached as Exhibit A.

19. Like Plaintiff, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach on or about January 8, 2025.

20. Defendant BayMark Health Services, Inc. is a Delaware corporation with its principal place of business located at 1720 Lakepointe Drive, Suite 117, Lewisville, TX 75057-6425. The registered agent for service of process is CT Corporation System, 1999 Bryan St., Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's

state of citizenship. Defendant is a citizen of Texas.

22. This Court has personal jurisdiction over the parties in this case. Defendant BayMark conducts business in the Sherman Division of the Eastern District of Texas and is a citizen of this District by virtue of having its principal place of business located in this District. Accordingly, this Court has general personal jurisdiction over Defendant. Likewise, because the breach which is at the core of this litigation occurred in the Sherman Division of the Eastern District of Texas, thereby impacting Plaintiff, this Court has specific personal jurisdiction over Plaintiff.

23. Venue is proper in the Sherman Division of the Eastern District of Texas under 28 U.S.C. §1391(b) because BayMark maintains a headquarters and principal place of business is in the Sherman Division of the Eastern District of Texas.

FACTUAL ALLEGATIONS

Defendant's Business

24. Defendant BayMark was founded in 2015 and represents itself as "one of the largest addiction treatment services in the US, operating roughly 200 facilities and over 380 programs in 35 states, and treating more than 70,000 patients every day."[4]

25. Defendant provides a complete range of "comprehensive addiction treatment programs to deliver medically supervised services for adults in a variety of modalities and settings. As the largest specialty healthcare organization in North America addressing substance use disorders, we provide a continuum of care."[5]

26. For the purposes of this Class Action Complaint, all of Defendant's associated locations will be referred to collectively as "Defendant."

[4] https://baymark.com/ (last visited February 13, 2025).
[5] *Id.*

27. In the ordinary course of receiving medical care services from Defendant, each patient must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as their:

- Name, address, phone number, and email address;
- Date of birth;
- Social Security number;
- Marital status;
- Employer with contact information;
- Primary and secondary insurance policy holders' name, and address;
- Demographic information;
- Driver's license or state or federal identification;
- Information relating to the individual's medical and medical history;
- Insurance information and coverage; and
- Banking and/or credit card information.

28. Defendant also creates and stores medical records and other protected health information for its patients, records of treatments and diagnoses.

29. Upon information and belief, Defendant's HIPAA Notice of Privacy Practices ("Privacy Policy") is provided to every patient both prior to receiving treatment and upon request.[6] Defendant's Privacy Notice makes clear that Defendant understands that its patients' Private Information is personal and must be protected by law.

30. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in

[6] https://baymark.com/privacy-practices/ (last visited February 13, 2025).

compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA").

31. Yet, through its failure to properly secure Plaintiff's and Class Members' Private Information, Defendant failed to meet its own promises of patient privacy.

32. The patient information held by Defendant in its computer system and network included Plaintiff's and Class Members' highly sensitive Private Information.

The Data Breach

33. A data breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

34. According to Defendant's website Notice, it learned of a cyberattack on its computer systems on or about October 11, 2024, when a cyberattack took many of Defendant's networked systems offline, adversely affecting patient treatment, scheduling, and the ability to access patient histories.[7]

35. Defendant notified Department of Health and Human Services ("HHS") of the Data Breach on or about January 8, 2025, listing thousands of individuals affected.

36. Since the Data Breach, according to cybersecurity news sources, at least one ransomware group, Ransomhub, has claimed responsibility for the attack.[8] Ransomhub claimed the theft of a massive 1.5 terabytes of data from BayMark's systems. The group has since made the allegedly stolen data publicly available.[9]

37. Ransomhub is one of the most active hackers, having hacked over 63 companies

[7] *See* n.1, *supra*.
[8] . https://www.hipaajournal.com/baymark-health-services-data-breach/ (last visited February 13, 2025).
[9] *Id.*

around the world since its inception during February 2024.[10] Ransomhub claims to have exfiltrated Plaintiffs' Private Information and then encrypted and published the files.[11]

38. Presently, however, Defendant has provided no public information on the ransom demand or payment. However, on its website, Ransomhub announced:

> One of the few companies from Texas that does not value its data. For a nominal fee, they could have not worried about anything, improved their network and protected themselves. But they chose the path of destroying their reputation, publishing sensitive data and publicizing it in the media.[12]

39. In January 2023, two years before the attack, HHS created a presentation specifically for healthcare providers and IT departments, warning entities like Defendant of the severe threats posed by cybercriminal groups.[13] Within the healthcare industry, the risk of a cyberattack is well-known and preventable with adequate security systems in place.

40. On or about January 8, 2025, months after Defendant learned that the Class Members' Private Information was attacked by cybercriminals, Defendant's patients began receiving their notices of the Data Breach informing them that its investigation determined that

[10] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub (last visited February 13, 2025).
[11] https://www.malwarebytes.com/blog/news/2025/01/baymark-health-services-sends-breach-notifications-after-ransomware-attack (last visited February 13, 2025).
[12] *Id.*
[13] https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf (last visited February 13, 2025).

their Private Information was accessed.

41. Defendant's notice letters list time-consuming, generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Also, Plaintiff would have to affirmatively contact a call center number with any questions. Defendant offered one year of credit monitoring for members of the class and Defendant offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Defendant sent a similar generic letter to all other individuals affected by the Data Breach.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

43. Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

44. Defendant had obligations created by HIPAA, FTCA, contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

45. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach was a
Foreseeable Risk of which Defendant was on Notice.

46. It is well known that PII and PHI, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Defendant, are well-aware of the risk of being targeted by cybercriminals.

47. Individuals place a high value on the privacy of their PII and PHI. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of uncompensated lost time trying to fight against the impact of identity theft.

48. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[14]

49. Individuals, like Plaintiff and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing one's DNA for hacker's purposes.

50. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

51. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state

[14] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085) available at: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited February 13, 2025).

motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So, using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[15]

52. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches from 2020. Over the next two years, in a poll of security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable cases will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[16]

53. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

54. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [17] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target

[15] https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited February 13, 2025).
[16] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited February 13, 2025).
[17] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited February 13, 2025).

more victims and offers an incentive for others to get involved in this type of illegal activity."[18]

55. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII and PHI private and secure, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiff and the proposed Class from being compromised.

Data Breaches are Rampant in Healthcare.

56. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

57. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[19]

58. More than 144 million Americans' medical information was stolen or exposed during 2024.[20] This represents the continuation of record-breaking health care data breaches in the last several years.[21]

59. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly

[18] *Id.*
[19] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited February 13, 2025).
[20] *See* n.11, *supra*.
[21] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited February 13, 2025).

detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[22]

60. The HIPAA Journal article goes on to explain that patient records, like those stolen from Defendant, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[23]

61. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

62. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[24]

63. HHS data shows more than 39 million patients' information was exposed in the first half of 2023 in nearly 300 incidents and that healthcare beaches have doubled between 2020 and 2023, according to records compiled from HHS data by Health IT Security.[25]

64. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In

---

[22] *Id.*
[23] *Id.*
[24] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited February 13, 2025).
[25] https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (last visited February 13, 2025).

fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[26]

65. The significant increase in attacks in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant.

Defendant Failed to Comply with FTC Guidelines.

66. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

67. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[27] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[28]

68. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

[26] https://www.ahu.edu/blog/data-security-in-healthcare (last visited February 13, 2025).
[27] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited February 13, 2025).
[28] *Id*.

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

69. The FTC has brought enforcement actions against businesses, like that of Defendant, for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

71. Defendant failed to properly implement basic data security practices.

72. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

73. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

74. As shown above, experts studying cyber security routinely identify healthcare

providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

75. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; utilizing strong passwords; creating multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data, and; limiting which employees can access sensitive data.

76. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

77. Upon information and belief Defendant failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

78. These frameworks are existing and applicable industry standards in the healthcare industry, yet Defendant failed to comply with these accepted standards, thereby opening the door to and failing to thwart the Data Breach.

Defendant's Conduct Violates HIPAA.

79. HIPAA requires covered entities such as Defendant to protect against reasonably

anticipated threats to the security of sensitive patient health information (PHI).

80. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

81. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

82. A Data Breach, such as the one Defendant experienced, is considered a breach under the HIPAA rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.

83. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate its failure to comply with safeguards mandated by HIPAA.

Defendant Breached its Obligations to Plaintiff and Class.

84. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its patients' data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §

164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures regarding data security, as well as PHI, as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

85. As the result of maintaining its computer systems in manner that required security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing the ransomware virus, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

86. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Put Consumers at an Increased Risk Of Fraud and Identify Theft

87. Data Breaches such as the one Plaintiff and Class Members experienced cause significant disruption to the overall daily lives of victims affected by the attack.

88. In 2019, the United States Government Accountability Office released a report addressing the steps consumers can take after a data breach.[29] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiff and Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

89. The GAO has long recognized that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

90. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[30]

91. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

92. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the

[29] https://www.gao.gov/assets/gao-19-230.pdf (last visited February 13, 2025).
[30] *See* https://www.identitytheft.gov/Steps (last visited February 13, 2025).

victim's information.

93. Theft of Private Information is also gravely serious. PII/PHI is valuable property.[31]

94. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to GAO:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See 2007 GAO Report, at p. 29.

95. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

96. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. This is evidenced by the fraud that has already taken place in Plaintiff Corralejo's case, as discussed in further detail below. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

97. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via

[31] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[32]

98. Furthermore, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[33] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[34] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

99. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

100. This data, as one would expect, commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

---

[32] https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf at 2 (citations omitted) (last visited February 13, 2025).
[33] *Identity Theft and Your Social Security Number*, Social Security Administration (last visited February 13, 2025). (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited February 13, 2025).
[34] *Id.* at 4.
[35] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited February 13, 2025).

information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[36]

101. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

PLAINTIFF'S EXPERIENCES

Plaintiff Carole Corralejo

102. Plaintiff Corralejo is and was Defendant's patient at all times relevant to this Complaint. Plaintiff Corralejo received a Notice of Data Breach Letter, related to Defendant's Data Breach that is dated January 8, 2025.

103. The Notice Letter that Plaintiff received does not explain exactly which parts of her PII and PHI were accessed and taken but instead generically states that the files contained her name, "date of birth, dates of service, medical record number, patient account number, medical treatment/diagnosis information, and health insurance policy number."

104. Plaintiff Corralejo is especially alarmed by the vagueness in the Notice Letter regarding her stolen extremely private medical information, including her PII/PHI, as among the breached data on Defendant's computer system.

105. Since the Data Breach, Plaintiff Corralejo has tried to mitigate the damage by

[36] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited February 13, 2025).

changing her passwords, contacting the credit bureaus as Defendant instructed, and monitoring her financial accounts for about 2 and a half hours per week. This is more time than she spent prior to learning of the Defendant's Data Breach. Having to do this every week not only wastes her time because of Defendant's negligence, but it also causes her great anxiety.

106. Soon after the Data Breach, Plaintiff Corralejo began receiving an excessive number of spam calls on the same cell phone number provided to Defendant on her records. These calls are a distraction, must be deleted, and waste time each day. Given the timing of the Data Breach, she believes that the calls are related to her stolen PII.

107. Plaintiff Corralejo is aware that cybercriminals often sell Private Information, and once stolen, it is likely to be abused months or even years after Defendant's Data Breach.

108. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered uncompensated lost time, annoyance, interference, and inconvenience because of the Data Breach.

109. Plaintiff has experienced anxiety and increased concerns arising from the fact that her PII has been or will be misused and from the loss of her privacy.

110. The risk is not hypothetical. Here, a known hacking group intentionally stole the data, misused it, threatened to publish, or has published it on the Dark Web, and the sensitive information, including names and Social Security numbers, is the type that could be used to perpetrate identity theft or fraud.

111. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Future identity theft monitoring is

reasonable and necessary, and such services will include future costs and expenses.

112. Plaintiff has a continuing interest in ensuring that her PII which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

113. Had Plaintiff Corralejo been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her PII and PHI.

PLAINTIFF'S AND CLASS MEMBERS' COMMON INJURIES

114. To date, Defendant has done absolutely nothing to compensate Plaintiff and Class Members for the damages they sustained in the Data Breach.

115. Defendant offered only one year of credit monitoring services to class members.

116. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for its unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, out of pocket costs, and the time they are required to spend attempting to mitigate their injuries.

117. Furthermore, Defendant's failure to safeguard Plaintiff's and Class Members' Private Information, places the burden squarely on Plaintiff and the Class, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts and omissions resulting in the Data Breach. Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

118. Plaintiff and Class Members have been damaged by the compromise and exfiltration, by cyber-criminals, of their Private Information as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

119. Plaintiff and Class Members were damaged in that their Private Information is now in the hands of cyber criminals being sold and potentially for sale for years into the future.

120. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft, especially in light of the actual fraudulent misuse of the Private Information that has already taken place, as alleged herein.

121. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

122. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

123. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

124. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

125. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

126. Plaintiff and Class Members have suffered or will suffer actual injury as a direct

result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

127. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from

further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information as well as health information is not accessible online and that access to such data is password-protected.

128. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

129. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of PII and PHI. Early notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach ***since November 5, 2024*** and did not notify the victims until January 8, 2025. Yet Defendant offered no explanation of purpose for the delay. This delay violates HIPAA and other notification requirements and increased the injuries to Plaintiff and Class.

CLASS ACTION ALLEGATIONS

130. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons whose Private Information was compromised as a result of the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about January 8, 2025 (the "Class" or "Class Members").

131. Plaintiff also seeks certification of a California Subclass as defined below:

> California Subclass: All individuals residing in California whose PII was submitted to Defendant or Defendant's affiliates and/or whose PII was compromised because of the data breach(es) by Defendant, including all those who received a Notice of the Data Breach (the "California Subclass").

132. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

133. This proposed Class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the Class definition in an amended pleading or when she moves for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

134. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiff is informed and believes, and thereon alleges, that there are at minimum, over a thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through BayMark's records, including but not limited to the files implicated in the Data Breach.

135. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether BayMark had a duty to protect Plaintiff's and Class members' PII;

b. Whether BayMark was negligent in collecting and storing Plaintiff's and Class members' PII, and breached its duties thereby;

c. Whether BayMark breached its fiduciary duty to Plaintiff and the Class;

d. Whether BayMark breached its duty of confidence to Plaintiff and the Class;

e. Whether BayMark violated its own Privacy Practices;

f. Whether BayMark entered a contract implied in fact with Plaintiff and the Class;

g. Whether BayMark breached that contract by failing to adequately safeguard

Plaintiff's and Class members' PII;

h. Whether BayMark was unjustly enriched;

i. Whether Plaintiff and Class members are entitled to damages as a result of BayMark's wrongful conduct; and

j. Whether Plaintiff and Class members are entitled to restitution as a result of BayMark's wrongful conduct.

136. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in BayMark's System, each having their PII exposed and/or accessed by an unauthorized third party.

137. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

138. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

139. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common

questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for BayMark. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

140. BayMark has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

141. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether BayMark failed to timely and adequately notify the public of the Data Breach;

b. Whether BayMark owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether BayMark's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether BayMark's failure to institute adequate protective security measures amounted to negligence;

e. Whether BayMark failed to take commercially reasonable steps to

safeguard consumers' and employees' PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

142. Finally, all members of the proposed Class are readily ascertainable. BayMark has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and Class Members)

143. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

144. Defendant required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare/medical services and/or employment.

145. By collecting and storing this data in Defendant's computer network and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer network—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

146. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the

Private Information.

147. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

148. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

149. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

150. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

151. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to

safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

152. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

153. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

154. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

155. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

156. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide

adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

157. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

158. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

159. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

160. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

161. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

162. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

163. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

164. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

165. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and Class Members)

166. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

167. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Defendant in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

168. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its patients. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

169. In the Privacy Policy, Defendant commits to protecting the privacy and security of private information and promises to never share Plaintiff's and Class Members' Private Information except under certain limited circumstances.

170. Plaintiff and Class Members fully performed their obligations under their contracts with Defendant.

171. However, Defendant did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Defendant breached its contracts with Plaintiff and Class Members.

172. Defendant allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, Defendant breached the Privacy Policy with Plaintiff and Class Members.

173. Defendant's failure to satisfy its confidentiality and privacy obligations, specifically those arising under the FTCA, HIPAA, and applicable industry standards, resulted in Defendant providing services to Plaintiff and Class Members that were of a diminished value.

174. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiff and Class Members.

175. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

176. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiff and Class Members for a period of at least three years.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and Class Members)

177. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

178. This Claim is pleaded in the alternative to Count III above.

179. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for Defendant's medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

180. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

181. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

182. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

183. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

184. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

185. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

186. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

187. As a direct and proximate result of Defendant's breach of the implied contracts,

Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

188. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

189. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class Members.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and Class Members)

190. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

191. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members: (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

192. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its current and former patients to keep secure their Private Information.

193. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give detailed notice of the Data Breach to Plaintiff and Class

in a reasonable and practicable period of time.

194. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

195. Defendant breached its fiduciary duty owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

196. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

197. As a direct and proximate result of Defendant's breaches of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

198. As a direct and proximate result of Defendant's breach of its fiduciary duty,

Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and Class Members)

199. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

200. Plaintiff brings this claim individually and on behalf of all Class Members.

201. This Claim is pleaded in the alternative to Counts III and IV a above.

202. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

203. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

204. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

205. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

206. In particular, Defendant enriched itself by saving the costs it reasonably should

have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

207. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

208. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

209. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

210. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

211. Plaintiff and Class Members have no adequate remedy at law.

212. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private

Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

213. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

214. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT VII
Invasion of Privacy
(On Behalf of Plaintiff and Class Members)

215. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

216. Plaintiff and Class Members had a legitimate expectation of privacy in their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

217. Defendant owed a duty to Plaintiff and Class Members to keep their Private

Information confidential.

218. Defendant failed to protect such information and permitted unknown third parties to exfiltrate Plaintiff's and Class Members' Private Information.

219. The unauthorized access to, exfiltration and publication of Plaintiff and Class Members' Private Information is highly offensive to a reasonable person.

220. The Data Breach constituted an intrusion into a place or thing, which is private, and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendant as part of their use of Defendant's services, but privately, with the intention that Private Information be kept confidential and be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

221. The Data Breach at the hands of the Defendant constitutes an intentional interference with the Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

222. Defendant acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its information security practices were inadequate and insufficient.

223. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

224. Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven

at trial.

225. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all Class Members.

COUNT VIII
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiff and Class Members)

226. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

227. Plaintiff brings this claim individually and on behalf of the Class.

228. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

229. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their PII. Plaintiff and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

230. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

231. Defendant still possess Plaintiff's and Class members' PII.

232. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiff's and Class members' PII.

233. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

234. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at BayMark. The risk of another such breach is real, immediate, and substantial.

235. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at BayMark, Plaintiff and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

236. Issuance of the requested injunction will not compromise the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at BayMark, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PII would be further compromised.

237. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that BayMark implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on BayMark's systems on a periodic basis, and ordering BayMark to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

COUNT IX
Violation of California's Unfair Competition Law ("UCL")
Cal Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff Corralejo and the California Subclass)

238. Plaintiff Corralejo restates and realleges the preceding allegations above as if fully alleged herein.

239. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

240. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

241. Defendant stored Plaintiff Corralejo and California Subclass Members' PII in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff Corralejo and the California Subclass's PII secure so as to prevent the loss or misuse of that PII.

242. Defendant failed to disclose to Plaintiff Corralejo and the California Subclass that their PII was not secure. However, Plaintiff Corralejo and the California Subclass were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff Corralejo and the California Subclass on notice that their PII was not secure, which Defendant had a duty to disclose.

243. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff Corralejo and the California Subclass' nonencrypted and nonredacted PII.

244. Had Defendant complied with these requirements, Plaintiff Corralejo and the California Subclass would not have suffered damage related to the data breach.

245. Defendant's conduct was unlawful, in that it violated the CCPA.

246. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

247. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

248. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

249. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

250. Instead, Defendant made Plaintiff Corralejo and California Subclass Members' PII accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff Corralejo and the California Subclass to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

251. As a result of those unlawful and unfair business practices, Plaintiff Corralejo and the California Subclass suffered an injury-in-fact and lost money or property.

252. The injuries to Plaintiff Corralejo and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all the circumstances.

253. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

254. Therefore, Plaintiff Corralejo and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT X
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiff Corralejo and the California Subclass)

255. Plaintiff Corralejo restates and realleges the preceding allegations above as if fully alleged herein.

256. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.*

257. The Data Breach constitutes a "breach of the security system" of Defendant.

258. An unauthorized person acquired Plaintiff Corralejo's and the California Subclass Members' unencrypted PII.

259. Defendant knew that an unauthorized person had acquired Plaintiff Corralejo's and California Subclass Members' personal, unencrypted PII but waited over three months to notify them. Given the severity of the Data Breach, waiting over three months was an unreasonable delay.

260. Defendant's unreasonable delay prevented Plaintiff Corralejo and the California Subclass from taking appropriate measures from protecting themselves against harm.

261. Because Plaintiff Corralejo and the California Subclass were unable to protect themselves, they suffered incrementally increased damage that they would not have suffered with timelier notice.

262. Plaintiff Corralejo and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and her counsel as Class Counsel;

b. For equitable relief enjoining BayMark from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling BayMark to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose

with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of BayMark's wrongful conduct;

e. Ordering BayMark to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 20, 2025

Respectfully submitted,

/s/ Joe Kendall
Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214.744.3000
Facsimile: 214.744.3015
jkendall@kendalllawgroup.com

Liberato P. Verderame*
Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newtown, PA 18940

T: (215) 867-2399
medelson@edelson-law.com
lverderame@edelson-law.com

Jeffrey S. Goldenberg*
Goldenberg Schneider, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
T: (513) 345-8291
jgoldenberg@gs-legal.com

Attorneys for Plaintiff and the Putative Class

* *Pro hac vice forthcoming*

EXHIBIT A

BayMark Health Services
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

8 1 1859 **********AUTO**ALL FOR AADC 945
Carole Corralejo
[redacted]

January 8, 2025

Dear Carole Corralejo,

BayMark Health Services, Inc. ("BayMark"), as the parent company of various healthcare facilities, provides administrative services to BAART Antioch (the Facility). We are writing to notify you about an incident that involved some of your information related to some of the services you received from the Facility. This letter explains the incident and the measures we have taken.

What Happened?
On October 11, 2024, we learned of an incident that disrupted the operations of some of our IT systems. We immediately took steps to secure our systems, launched an investigation with the assistance of third-party forensic experts, and notified law enforcement. Our investigation determined that an unauthorized party accessed some of the files on BayMark's systems between September 24, 2024 and October 14, 2024. We then initiated a review and analysis of those files.

What Information Was Involved?
On November 5, 2024, we determined that these files contained information that varied per patient but could have included your name and one or more of the following: Social Security number, driver's license number, date of birth, services received, dates of service, insurance information, treating provider, and treatment and/or diagnostic information.

What We Are Doing.
We are notifying you of this incident to assure you that we take this matter very seriously. To help prevent something like this from happening again, we have implemented additional safeguards and technical security measures to further protect and monitor our systems.

We are offering you a one-year complimentary membership to Equifax Complete™ Premier. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. Equifax Complete™ Premier is completely free to you and enrolling in this program will not hurt your credit score. For more information, including instructions on how to activate your complimentary membership, please see the pages that follow this letter.

What You Can Do.
We encourage you to sign up for the complimentary credit monitoring services. Additionally, it is always a good idea to remain vigilant and review statements you receive for suspicious activity. Please review the enclosed *Additional Steps You Can Take,* which contains information about what you can do to safeguard against possible misuse of your information.

JS 44 (Rev. 07/16)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

CAROLE CORRALEJO, Individually and on behalf of those similary situated

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Joe Kendall, Kendall Law Group, PLLC, 3811 Turtle Creek Blvd., Suite 825, Dallas, TX 75219; 214/744-3000

DEFENDANTS

BAYMARK HEALTH SERVICES, INC.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
02/20/2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Joe Kendall

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____